Affaires C-511/18 et C-512/18

La Quadrature du Net

Le 27 novembre 2018

Table des matières

1 Introduction

1 Le Conseil d'État a transmis à la Cour de justice de l'Union européenne cinq questions préjudicielles.

2 Trois de ces questions concernent la conformité au droit de l'Union européenne des dispositions françaises qui imposent aux intermédiaires techniques de conserver pendant un an des **données de connexion** concernant l'ensemble de leurs utilisateurs. Il s'agit des deux questions transmises dans l'affaire C-512/18 et de la première question transmise dans l'affaire C-511/18. Elles sont traitées par la Fédration FDN et Igwan dans leurs propres écritures.

3 Deux autres questions concernent la conformité au droit de l'Union européenne du cadre, plus large, des **activités étatiques de surveillance**, couvrant les mesures directement mises en œuvre par l'État ainsi que l'effectivité des recours prévus contre ces mesures. Il s'agit des deuxième et troisième questions transmises dans l'affaire C-511/18. Elles seront traitées dans les présentes écritures.

4 Par ces deux questions, le Conseil d'État demande à la Cour de préciser les conditions dans lesquelles l'État peut directement surveiller la population (section 2) ou limiter les voies de recours ouvertes à la population (section 3 page 15).

2 Les conditions de mise en œuvre de la surveillance

5 En substance, le Conseil d'État demande à la Cour de définir les conditions dans lesquelles la directive 2002/58 et la Charte permettent aux États de collecter directement des données couvertes par le secret des correspondances, notamment en interceptant des données de connexion ou de localisation (deuxième question dans l'affaire C-511/18).

6 Répondre à cette question demande d'abord de définir clairement le cadre juridique applicable (section 2.1 page suivante) pour ensuite préciser les garanties prévues par le droit de l'Union s'agissant :

- des finalités pouvant être poursuivies (section 2.2 page 6) ;
- des données pouvant être collectées (section 2.3 page 7) ;
- des services pouvant réaliser les mesures (section 2.4 page 11)
- de l'utilisation des données après leur collecte (section 2.5 page 11) ; et
- du contrôle indépendant de ces mesures (section 2.6 page 12).

7 Pour répondre de façon précise et utile à la question transmise par le Conseil d'État, chacune de ces règles sera comparée aux mesures de surveillance que l'administration peut réaliser en droit français. Pour la clarté du propos, il faut d'abord présenter sommairement certaines de ces mesures.

8 Le code de la sécurité intérieure (CSI) permet à l'administration, sur simple autorisation du Premier ministre, d'intercepter des communications électroniques (article L852-1), de collecter des données de connexion et de localisation auprès des opérateurs et hébergeurs (article L851-1), d'exiger aux opérateurs de lui transmettre en temps réel des données

de localisation (article L851-4), de dévoyer le réseau pour intercepter des données de connexion, typiquement à l'aide d'IMSI-catcher (article L851-6) et de pirater un terminal informatique (à distance ou en s'immisçant dans un lieu privé) pour accéder aux données qui sont entrées, affichées ou enregistrées sur ce terminal (article L853-2). Ces mesures peuvent viser toute personne (suspectée ou non) dont la surveillance est susceptible de révéler des informations utiles à la poursuite de l'une des nombreuses finalités prévues par le CSI.

9 De plus, pour ces mêmes finalités, et toujours sur simple autorisation du Premier ministre, l'administration peut intercepter sur un ou plusieurs réseaux l'ensemble des communications émises vers ou reçues depuis l'extérieur du territoire français, notamment vers ou depuis un autre État membre de l'Union (article L854-2). Une fois collectées, l'administration peut analyser au moyen de « *traitements automatisés* » l'ensemble des données de connexion interceptées. Enfin, elle peut exploiter le contenu de l'ensemble des communications qui sont en lien avec les « zones géographiques » ou les « groupes de personnes » visés par l'autorisation du Premier ministre.

10 À ces mesures d'intrusion informatique s'ajoute la possibilité pour l'administration, dans les mêmes conditions et pour les mêmes finalités, de capter des images et des conversations privées, à distance ou en posant micros et caméras dans des lieux privés (article L853-1), ou de poser des dispositifs permettant de suivre la localisation de personnes et d'objets, notamment en entrant dans des lieux privés (article L853-1).

11 Enfin et, cette fois-ci, pour la seule lutte contre le terrorisme, l'administration peut recueillir en temps réel des données de connexion (article L851-2) et placer sur les réseaux des dispositifs interceptant et traitant automatiquement les données acheminées afin de « *détecter des connexions susceptibles de révéler une menace terroriste* » (L851-3).

2.1 Le cadre juridique européen de la surveillance d'État

12 La Cour de justice a précisé que « *la protection de la confidentialité des communications électroniques et des données relatives au trafic y afférentes, garantie à l'article 5, paragraphe 1, de la directive 2002/58, s'applique aux mesures prises par toutes les personnes autres que les utilisateurs, qu'il s'agisse de personnes ou d'entités privées ou d'entités étatiques* » (Tele2[1], § 77). Cet article 5 pose l'interdiction de principe « *d'écouter, d'intercepter, de stocker les communications et les données relatives au trafic y afférentes, ou de les soumettre à tout autre moyen d'interception ou de surveillance* » ainsi que d'obtenir « *l'accès à des informations déjà stockées, dans l'équipement terminal d'un abonné ou d'un utilisateur* ».

13 L'article 15 de la directive 2002/58 permet aux États membres de prendre certaines mesures dérogeant à cet article 5, notamment « pour sauvegarder la sécurité nationale » ou « la sécurité publique, ou assurer la prévention, la recherche, la détection et la poursuite d'infractions pénales », mais seulement si ces mesures « sont prises dans le respect des principes généraux du droit communautaire ».

14 En France, la quasi-totalité des mesures autorisées par le CSI sont des dérogations à

1. CJUE, grande chambre, 21 décembre 2016, Tele2 Sverige, Watson et autres, C-2013/15, C-698/15

l'article 5 de la directive 2002/58 : interception des communications (article L852-1), collecte de données de connexion et de localisation (article L851-1), notamment en temps réel (articles L851-4 et L851-2), dispositifs de type IMSI-catcher (article L851-6), piratage informatique (article L853-2), dispositifs d'analyse automatique du réseau (article L851-3) et surveillance internationale (article L854-1).

15 Les « principes généraux du droit communautaire » qu'un État doit respecter pour déroger à l'article 5 de la directive 2002/58 en application de son article 15 sont définis tant par la Charte (2.1.1) que par le droit dérivé (2.1.2).

2.1.1 La Charte

16 De façon générale, la Cour de justice a précisé que, parmi ces principes, « *figurent les principes généraux et les droits fondamentaux qui sont désormais garantis par la Charte* » (Tele2, § 91). Ainsi, la Cour de justice a reconnu que l'article 15 de la directive 2002/58 « *présuppose nécessairement que les mesures nationales qui y sont visées [...] relèvent du champ d'application de cette même directive, puisque cette dernière n'autorise expressément les États membres à les adopter que dans le respect des conditions qu'elle prévoit* » (Tele2, § 73). La Cour conclut que les États membres doivent respecter la Charte, et notamment ses articles 7 et 8, lorsqu'ils prennent des mesures poursuivant n'importe laquelle des finalités visées à l'article 15 (sécurité nationale, lutte contre les infractions, etc.).

17 Ce raisonnement est une simple application du principe général reconnu par la Cour de justice selon lequel « *l'emploi, par un État membre, d'exceptions prévues par le droit de l'Union pour justifier une entrave à une liberté fondamentale garantie par le traité doit, dès lors, être considéré [...] comme « mettant en œuvre le droit de l'Union », au sens de l'article 51, paragraphe 1, de la Charte* », et comme devant donc respecter celle-ci (arrêt Pfleger, C-390/12, du 30 avril 2014, point 36).

2.1.2 Le droit dérivé

18 De façon plus spécifique, les « principes généraux » visés à l'article 15 de la directive 2002/58 sont aussi précisés par deux autres normes européennes : le RGPD et la directive 2016/680.

a. Le RGPD

19 Tel que le rappelle l'article 1, §2, de la directive 2002/58, « *les dispositions de la présente directive précisent et complètent la directive 95/46/CE* ». Pour bénéficier de la dérogation prévue à l'article 15, les États membres doivent donc respecter les principes généraux reconnus par le Règlement général sur la protection des données personnelles (RGPD), qui a remplacé la directive 95/46/CE, chaque fois que leur activité est soumise aux dispositions de ce règlement.

20 Au regard de l'article 2 du RGPD, ses dispositions s'appliquent à tout traitement de données personnelles réalisé par un État membre à l'exception de trois catégories de

traitements : ceux réalisés dans le cadre de la sécurité commune de l'Union, ceux visant à prévenir, détecter, poursuivre ou sanctionner des infractions pénales et ceux visant à sauvegarder la sécurité nationale.

21 Ainsi, par exemple, tout État membre doit respecter les principes généraux du RGPD lorsque, usant de la dérogation prévue à l'article 15 de la directive 2002/58, il intercepte des communications, collecte des données de connexion ou pirate un terminal informatique à des fins de surveillance économique, industrielle ou scientifique ou afin de mettre en œuvre sa politique étrangère.

b. La directive 2016/680

22 Les « principes généraux » du droit de l'Union en matière de surveillance policière ont précisément fait l'objet d'une directive pour les définir : la directive 2016/680. Au regard de son article 1, les dispositions de cette directive s'appliquent à tout traitement de données personnelles réalisé par un État membre « *à des fins de prévention et de détection des infractions pénales, d'enquêtes et de poursuites en la matière ou d'exécution de sanctions pénales, y compris la protection contre les menaces pour la sécurité publique et la prévention de telles menaces* ». Ainsi, par exemple, tout État membre doit respecter les principes généraux de cette directive lorsqu'il intercepte des communications, collecte des données de connexion ou pirate un terminal informatique afin de lutter contre le trafic de stupéfiants ou le terrorisme.

23 À noter que, contrairement, au RGPD, le cadre de la sécurité commune de l'Union n'est pas exclu du champ d'application des dispositions de cette directive. Toutefois, ici encore, ces dispositions ne s'appliquent pas en tant que telles aux traitements qui visent à sauvegarder la sécurité nationale : cette directive, tout comme le RGPD et la directive 2002/58, exige simplement que ces traitements respectent les garanties reconnues par la Charte.

24 **En conclusion** et pour résumer, l'ensemble des traitements réalisés par un État membre sont soumis au RGPD ou à la directive 2016/680, selon la finalité poursuivie, ainsi qu'à la Charte, quelque soit la finalité poursuivie — y compris lorsque cette finalité relève de la sécurité nationale.

25 En pratique, la sécurité nationale est une finalité poursuivie de façon marginale par l'administration française. En 2015, dans son 23ème rapport d'activité, la Commission nationale de contrôle des interceptions de sécurité (CNCIS, l'autorité notifiée de la mise en place des techniques de renseignement jusqu'à 2015) précisait que, en matière d'interception de sécurité, « la prévention de la criminalité et délinquance organisées reste le premier motif des demandes initiales avec 48%, suivie de la prévention du terrorisme avec 38% [...] et de **la sécurité nationale avec 12%** ».

26 Par ailleurs, il faut rappeler, tel que le CNCIS le faisait ci-dessus, que la lutte contre le terrorisme ne relève pas du domaine de la sécurité nationale. Ce domaine est défini par l'article 4, §2, du Traité sur l'Union européenne comme relevant « de la seule responsabilité de chaque État membre » alors que la lutte contre le terrorisme entre dans les compétences législatives de l'Union.

27 En effet, l'article 83, §1, du Traité sur le fonctionnement de l'Union européenne prévoit que « le Parlement européen et le Conseil, statuant par voie de directives conformément

à la **procédure législative ordinaire**, peuvent établir des règles » dans les domaines suivants : « le **terrorisme**, la traite des êtres humains [...] ». À ce titre, l'Union a notamment adopté la directive 2017/541 « relative à la lutte contre le terrorisme » qui « énumère de manière exhaustive un certain nombre d'infractions graves, telles que les atteintes à la vie d'une personne, en tant qu'actes intentionnels pouvant être qualifiés d'infractions terroristes » (considérant 8). Les mesures de surveillance réalisées par l'État pour lutter contre le terrorisme doivent donc respecter l'ensemble des dispositions de la directive 2016/680.

2.2 Les finalités poursuivies

28 En interprétation de la Charte, le Cour de justice a précisé que les mesures de surveillance réalisées par les États membres doivent « *répondre à des critères objectifs, établissant un rapport entre les données à conserver et l'objectif poursuivi* » et « *s'avérer, en pratique, de nature à délimiter effectivement l'ampleur de la mesure et, par suite, le public concerné* » (Tele2, § 110). De plus, en matière de lutte contre les infractions, « *seule la lutte contre la criminalité grave est susceptible de justifier une telle mesure* » (Tele2, § 102).

29 En droit français, les mesures prévues par le CSI peuvent notamment être réalisées pour poursuivre les finalités suivantes :

- la défense des « intérêts majeurs de la **politique étrangère** » (CSI, L811-3, 2°), ces intérêts étant discrétionnairement définis par le Gouvernement ;
- « l'exécution des engagement **européens et internationaux** de la France » (CSI, L811-3, 2°), notamment l'application des normes de l'Union européenne sur l'agriculture, la pêche, les transports, l'emploi, la culture ou le tourisme ainsi que les accords internationaux tels que l'accord de Paris de 2015 sur le climat ou la Convention de Genève de 1931 sur le droit de timbre en matière de chèque ;
- la défense des « intérêts **économiques, industriels et scientifiques** de la France » (CSI, L811-3, 3°), qui permet l'espionnage industriel et scientifique ;
- les prévention des « violences collectives de nature à porter gravement atteinte à la paix publique » (CSI, L811-3, 5°, c), couvrant notamment la lutte contre les **manifestations**, même non-violentes, n'ayant pas été déclarées ou ayant fait l'objet d'une déclaration incomplète (voir la décision DC 2015-713 du Conseil constitutionnel français qui, à son considérant 10, renvoie aux articles 431-1 à 431-10 du code pénal pour définir cette finalité, notamment celle prévue à l'article 431-9 du code pénal) ;
- « la prévention de la criminalité et de la délinquance organisée » (CSI, L811-3, 6°), notamment la lutte contre l'acquisition illicite de **stupéfiants**, même par un individu seul qui n'agit pas en groupe (voir la décision DC 2015-713 du Conseil constitutionnel français qui renvoie aux infractions listées à l'article 706-73 du code de procédure pénale pour définir cette finalité, notamment celle prévue à l'article 222-37 du code pénal) ;

30 Un grand nombre de ces finalités sont particulièrement larges ou laissées à l'appréciation discrétionnaire de l'administration, ne répondant à aucun critère objectif permettant de délimiter effectivement l'ampleur des mesures de surveillance qu'elles autorisent. Il en va notamment de la défense des « intérêts majeurs de la politique étrangère », de «

l'exécution des engagements européens et internationaux » ou de la défense des « intérêts économiques, industriels et scientifiques » de la France.

31 D'autres finalités concernent la lutte contre des infractions qui ne relèvent pas de la criminalité grave. Il en va notamment de la lutte contre les manifestations non-déclarées ou l'acquisition de stupéfiants à titre individuel.

32 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, la Cour de justice doit déclarer comme étant contraires à celle-ci des dispositions nationales qui autorisent des dérogations à l'article 5 de la directive 2002/58 pour de telles finalités.

2.3 Les données collectées

33 Le droit de l'Union exige que, quelque soit la finalité poursuivie, les données collectées soient limitées au strict nécessaire. Cela implique de limiter le nombre de personnes visées à celles en lien avec la finalité poursuivie (section 2.3.1), à interdire toute surveillance de masse (section 2.3.2 page suivante) et à supprimer les données collectées inutilement (setion 2.3.3 page 10).

2.3.1 Le lien avec la finalité poursuivie

34 La Cour de justice a déclaré qu'une disposition nationale autorisant un État à collecter de données personnelles « *indépendamment d'un quelconque lien, à tout le moins indirect, avec le but poursuivi, ne saurait être considéré comme limité au strict nécessaire* » et, ainsi, comme conforme à la Charte (Tele2, § 119).

35 Ce principe général se retrouve tant dans le RGPD, qui prévoit que les données collectées doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées* » (article 5, §1, c), que dans la directive 2016/680, qui prévoit que ces données doivent être « *adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont traitées* » (article 4, §1, c).

36 De façon plus spécifique, la Cour de justice a précisé que « *un accès ne saurait, en principe, être accordé, en relation avec l'objectif de lutte contre la criminalité, qu'aux données de personnes soupçonnées de projeter, de commettre ou d'avoir commis une infraction grave ou encore d'être impliquées d'une manière ou d'une autre dans une telle infraction* » (même décision, même paragraphe). Ce n'est que *par exception* que la Cour nuance que, « *toutefois, dans des situations particulières, telles que celles dans lesquelles des intérêts vitaux de la sécurité nationale, de la défense ou de la sécurité publique sont menacés par des activités de terrorisme, l'accès aux données d'autres personnes pourrait également être accordé lorsqu'il existe des éléments objectifs permettant de considérer que ces données pourraient, dans un cas concret, apporter une contribution effective à la lutte contre de telles activités* » (Tele2, § 119).

37 En droit français, **cette exception devient la règle**. Toutes les mesures de surveillance autorisées par le CSI peuvent être réalisées contre des personnes qui ne participent à

aucune menace contre la finalité poursuivie. En effet, le CSI autorise des mesures visant toute personne dont la surveillance est susceptible de révéler des informations utiles à la poursuite de n'importe quelle finalité prévue à son article L811-3. Il en va ainsi lorsque, par exemple, une personne fait partie de la famille ou des collègues d'une autre personne soupçonnée de participer à une menace. Cette situation est la règle : **elle ne dépend d'aucune « situation particulière »** ou de certaines finalités limitées à des menaces particulières, contrairement à ce qu'exige le droit de l'Union.

38 Par exception, l'article L851-2 du CSI, qui permet à l'administration d'accéder en temps réel aux données de connexion pour lutter contre le terrorisme, est le seul article du CSI à délimiter le champ des personnes pouvant être visées par la mesure qu'il autorise. Il s'agit de toute « personne préalablement identifiée susceptible d'être en lien avec une menace » ainsi que, « lorsqu'il existe des raisons sérieuses de penser qu'une ou plusieurs personnes appartenant à l'entourage de la personne concernée par l'autorisation sont susceptibles de fournir des informations », de ces personnes. Toutes les autres mesures autorisées par le CSI ne prévoient pas une telle limitation - qui, d'ailleurs, ne limite pas la mesure à des « situations particulières » mais couvre n'importe quelle enquête anti-terroriste.

39 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, permettent des dérogations à l'article 5 de la directive 2002/58 pour, en toute circonstance, surveiller des personnes qui ne participent d'aucune façon à une menace contre un intérêt légitime défendu par l'État.

2.3.2 La surveillance de masse

40 La Cour de justice a déclaré qu'une « *réglementation permettant aux autorités publiques d'accéder de manière généralisée au contenu de communications électroniques doit être considérée comme portant atteinte au contenu essentiel du droit fondamental au respect de la vie privée, tel que garanti par l'article 7 de la Charte* » (Schrems [2], § 94).

41 De même, elle a reconnu que « *n'est pas limitée au strict nécessaire une réglementation qui autorise de manière généralisée la conservation de l'intégralité des données à caractère personnel de toutes les personnes dont les données ont été transférées depuis l'Union vers les États-Unis sans qu'aucune différenciation, limitation ou exception soit opérée en fonction de l'objectif poursuivi* » (même arrêt, § 93).

42 Naturellement, toute mesure de surveillance de masse est aussi contraire aux articles 5, §1, c, du RGPD et 4, §1, c de la directive 2016/680 cités ci-avant.

43 En droit français, deux dispositions prévoient des mesures de surveillance de masse.

44 **En premier lieu**, l'article L854-2 du CSI prévoit que le Premier ministre peut, pour poursuivre l'une des nombreuses finalités de l'article L811-3, autoriser son administration à **collecter et conserver l'intégralité des communications transférés** vers

2. CJUE, grande chambre, 6 octobre 2015, Schrems, C-362/14

ou depuis l'extérieur du territoire français. Il peut aussi autoriser l'exploitation et l'accès par traitement automatisé à l'intégralité des données de connexion ainsi collectées. S'agissant du contenu des communications interceptées, le Premier ministre peut autoriser l'administration à accéder et à exploiter l'ensemble des messages se référant à des « zones géographiques » entières.

45 Dans la loi française, rien n'empêche donc le Premier ministre d'autoriser son administration à lire l'ensemble des communications émises et reçues, par exemple, depuis l'Allemagne, le Moyen-Orient ou la « zone géographique » qui entoure la Cour de justice de l'Union, notamment pour assurer « *l'exécution des engagement européens* » de la France - finalité prévue à l'article L811-3.

46 **En second lieu**, l'article L851-3 du CSI prévoit que, en matière de lutte contre le terrorisme, le Premier ministre peut autoriser l'installation, sur un point d'un réseau, d'un dispositif interceptant et analysant automatiquement et en continu l'ensemble des messages passant par ce point.

47 Pour définir les données que peut analyser ce dispositif, l'article L851-3 opère un renvoi à la liste des données que les opérateurs et les hébergeurs ont, par ailleurs, l'obligation de conserver. L'article R851-5 du CSI précise la nature de ces données, indiquant notamment que les dispositifs d'analyse automatique peuvent traiter celles « relatives à l'identification et à l'authentification d'un utilisateur, d'une connexion, d'un réseau ou d'un service de communication au public en ligne ». Concrètement, cela peut notamment couvrir l'*adresse IP* des messages transmis, typiquement, mais aussi les **adresses e-mail**, les *pseudonymes* et les *adresses URL* des pages Web visitées. Ces deux dernières catégories de données relèvent directement du *contenu des communications* : il ne s'agit en rien d'informations nécessaires aux opérateurs de télécommunications pour assurer l'acheminement des messages sur les réseaux. La nature de ces données ne devrait toutefois pas altérer l'ampleur de l'ingérence permise par cette surveillance de masse puisque, comme l'a rappelé la Cour de justice, la surveillance du contenu des communications ou des données de connexion y afférentes posent des risques d'une égale gravité. * § Quoi qu'il en soit, et concrètement, selon les endroits où ces dispositifs sont installés, rien n'empêche le Premier Ministre d'autoriser la *surveillance automatisée de l'ensemble des communications de la population* d'un quartier, d'une région ou d'un pays, au fur et à mesure que les capacités de calcul de la France se développeront.

48 Enfin, et peu importe le nombre des personnes affectées par la surveillance internationale ou le dispositif d'analyse automatique du réseau, ces mesures visent des personnes qui ne présentent *aucun lien pré-existant avec une quelconque menace*, puisque l'objectif même de ces mesures est de révéler un tel lien. Ceci suffit à les rendre systématiquement contraires à l'interprétation que la Cour de justice donne de la Charte, telle qu'exposée ci-avant.

49 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, la Cour de justice doit déclarer comme étant contraires à celle-ci des dispositions nationales qui, telles que celles prévues en droit français, dérogent à l'article 5 de la directive 2002/58 pour collecter ou analyser les communications de l'ensemble d'une population au sein d'une zone géographique donnée.

2.3.3 Les données inutiles

50 Le principe de minimisation des données, imposé tant par la Cour de justice au regard de la Charte que par les articles 5 du RGPD et 4 de la directive 2016/680, exige aussi de s'assurer de la destruction des données collectées inutilement au regard de la finalité poursuivie. Or, en droit français, au contraire, la conservation des données inutiles est la règle.

51 L'article L851-6 du CSI, qui permet à l'administration de dévoyer le réseau afin d'intercepter des données de connexion, typiquement au moyen d'IMSI-catcher, permet une conservation jusqu'à 90 jours des données qui « *ne sont pas en rapport avec l'autorisation de mise en œuvre* ».

52 De façon plus générale, l'article L822-2, prévoit une conservation de *4 ans* de toutes les données de connexion interceptées et de *6 ans* pour le contenu des correspondances chiffrées, sans faire aucune distinction entre les données utiles ou non à la poursuite de la finalité qui en a justifié la collecte.

53 Certes, l'article L822-3 prévoit que « *les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite de ces finalités* », mais cette exigence ne concerne que les informations mises en forme (transcrites et extraites dans des fiches ou dossiers) et non les informations brutes qui sont considérées indépendamment par la loi sous la dénomination de « renseignements ». Cette distinction entre données brutes (« renseignement ») et données mises en forme (« transcriptions et extractions ») est clairement explicitée au début de l'article L822-3, qui précise que « *les renseignements ne peuvent être collectés, transcrits ou extraits pour d'autres finalités que celles mentionnées à l'article L. 811-3* ».

54 La situation est encore plus grave en matière de surveillance internationale. L'article L854-5 prévoit que, s'agissant des communications émises depuis ou vers l'extérieur du territoire français, le contenu des correspondances, même non-chiffrées, est conservé pendant 1 an et que les données de connexion le sont pendant 6 ans. Ici encore, l'article L854-6 se contente de prévoir la destruction des « transcriptions et extractions » inutiles pour la finalité poursuivie mais laisse possible la conservation pendant 1 ou 6 ans d'informations brutes inutiles.

55 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte et du principe de minimisation prévu par le RGPD et la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, dérogent à l'article 5 de la directive 2002/58 sans prévoir la suppression sans délai des données personnelles non-nécessaires à la finalité qui en a motivé la collecte.

56 De même, l'interprétation de la Charte, du RGPD et de la directive 2016/680 gagnera en clarté si la Cour de justice déclarait excessifs les délais de conservation ci-avant exposés.

2.4 Les services pouvant réaliser les mesures

57 La Cour de justice a déclaré contraire à la Charte une mesure de surveillance qui « *ne prévoit aucun critère objectif permettant de limiter le nombre de personnes disposant de l'autorisation d'accès et d'utilisation ultérieure des données* » (Digital Rights Ireland [3], § 62). Cette limitation est indispensable dans la mesure où les risques de dérives et d'abus des mesure de surveillance ainsi que la difficulté du contrôle que peut en faire une autorité indépendante sont proportionnels au nombre de personnes pouvant les mettre en œuvre.

58 En droit français, l'article L811-4 du CSI prévoit que le gouvernement, de son propre chef, « *désigne les services, autres que les services spécialisés de renseignement, relevant des ministres de la défense, de l'intérieur et de la justice ainsi que des ministres chargés de l'économie, du budget ou des douanes, qui peuvent être autorisés à recourir aux techniques* » prévues par ce code. Ainsi, aucune loi n'empêche le gouvernement d'étendre autant qu'il le souhaite le nombre des agents de son administration pouvant mettre en œuvre les mesures de renseignement, sans ce soucier d'augmenter les risques de dérive et les difficultés du contrôle indépendant.

59 En trois ans, le gouvernement a déjà pris un décret n° 2015-1639 du 11 décembre 2015 et décret n° 2017-36 du 16 janvier 2017 pour étendre considérablement le nombre de ses services (et donc de ses agents) pouvant recourir aux mesures de renseignement. En donner ici la liste, même sommaire, ne répondrait pas à la brièveté attendue par la Cour.

60 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, autorisent des mesures dérogeant à l'article 5 de la directive 2002/58 sans prévoir de critère objectif pour limiter le nombre de personnes pouvant réaliser ces mesures.

2.5 L'utilisation ultérieure des données

61 La Cour de justice reconnaît qu'est contraire à la Charte une mesure de surveillance qui « *ne prévoit aucun critère objectif permettant de délimiter l'accès des autorités nationales compétentes aux données et leur utilisation ultérieure* » à ce qui est strictement nécessaire (Digital Rights Ireland, § 60). L'article 5, §1, b, du RGPD reprend ce principe en prévoyant que les données personnelles doivent être « *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités* ». De même, l'article 4, §1, b, de la directive 2016/680 prévoit que les données personnelles sont « *collectées pour des finalités déterminées, explicites et légitimes et ne sont pas traitées d'une manière incompatible avec ces finalités* ».

62 À ce titre, la directive 2016/680 a été partiellement transposée au chapitre XIII de la loi n° 78-17 du 6 janvier 1978. Les articles 70-3 et 70-5 de cette loi prévoient que tout traitement de données personnelles réalisé par l'État à des fins « *de prévention et de détection des infractions pénales* » doit être « *prévu par une disposition législative ou*

3. CJUE, grande chambre, 8 avril 2014, Digital Rights Ireland et autres, C-293/12, C-594/12

réglementaire » qui, en principe, doit limiter l'utilisation des données à la finalité qui en a motivé la collecte (la lutte contre les infractions).

63 Pourtant, aucune disposition législative ou réglementaire française n'autorise ou ne définit les conditions d'utilisation des informations obtenues au moyen des techniques autorisées par le CSI. Le CSI n'encadre que les techniques de collecte, de transcription et d'extraction des renseignements, mais pas l'utilisation qui est faite des informations ainsi réunies. Autrement dit, en droit français, une fois que les renseignements ont été collectés, transcrits et extraits, pour être mis en forme de façon utilisable par les services (fiche, dossier), *aucun cadre juridique ne définit l'utilisation ultérieure* qui peut en être faite.

64 Tout au plus, l'article L822-3 prévoit que, s'agissant des renseignements collectés pour les finalités prévues à l'article L811-3, « *les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite de ces finalités* ». Mais cette disposition ne limite que la conservation des informations et, en aucun cas, leur utilisation. Par exemple, elle n'empêche pas qu'une fiche valablement conservé pendant 1 an à des fins de surveillance économique soit, pendant cette même durée, aussi utilisée pour des finalités politiques étrangères à celle-ci.

65 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, autorisent des mesures dérogeant à l'article 5 de la directive 2002/58 pour collecter des données personnelles sans définir les conditions d'utilisation ultérieure de ces données.

66 De même, le chapitre V du RGPD et de la directive 2016/680 impose aux États membres des conditions strictes pour transférer les données qu'ils ont recueilles à des États ne faisant pas partie de l'Union ou à une organisation internationale. En droit français, l'article 70-25 de la loi de 1978, où la directive 2016/680 a été partiellement transposée, exige que ce cadre soit repris par la disposition législative ou réglementaire qui autorise la mise en œuvre par l'État d'un traitement de données personnelles visant à lutter contre les infractions.

67 Pourtant, ici encore, puisque aucune disposition législative ou réglementaire n'encadre l'utilisation des informations obtenues au moyen des techniques autorisées par le CSI, leur transfert n'est soumis à *aucun cadre juridique*.

68 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, autorisent des mesures dérogeant à l'article 5 de la directive 2002/58 pour collecter des données personnelles sans définir les conditions de leur transfert hors Union ou à des organisations internationales.

2.6 Le contrôle indépendant

69 L'article 8, paragraphe 3, de la Charte prévoit que « le respect [des règles sur la protection des données] est soumis au contrôle d'une autorité indépendante ». La Cour de justice

en déduit que la mise en œuvre d'une mesure de surveillance par des autorités nationales doit être « subordonné[e] à un **contrôle préalable** effectué soit par une juridiction soit par une entité administrative indépendante, et que la décision de cette juridiction ou de cette entité intervienne à la suite d'une demande motivée de ces autorités » (Tele2, § 120).

70 Ce principe se traduit notamment à l'article 58 du RGPD qui exige que cette autorité de contrôle puisse accéder à toutes les données personnelles traitées et ordonner qu'un traitement soit mis en conformité à la loi ou prenne fin. De même, l'article 47 de la directive 2016/680 prévoit que « chaque autorité de contrôle dispose de pouvoirs d'enquête effectifs. Ces pouvoirs comprennent au moins celui d'obtenir du responsable du traitement ou du sous-traitant l'accès à toutes les données à caractère personnel qui sont traitées » et que « chaque autorité de contrôle dispose de pouvoirs effectifs en matière d'adoption de mesures correctrices ».

71 Ce contrôle doit intervenir au préalable, avant la collecte de données (a), et après, en contrôlant l'utilisation faite des données collectées (b). Il doit aussi s'opérer tout le long s'agissant des informations échangées avec des services étrangers (c).

2.6.1 Le contrôle de la collecte

72 En droit français, l'article L821-2 du CSI prévoit que la demande de mise en œuvre d'une technique de renseignement est formulée par le ministre de la défense, de l'intérieur, de la justice ou de l'économie au Premier Ministre, au nom des agents de leurs services qui la réclament. L'article L821-3 prévoit que la commission nationale de contrôle des techniques de renseignement (CNCTR), qui est l'entité indépendante du gouvernement sensée contrôler ces mesures, est uniquement notifiée de la demande d'autorisation adressée au Premier Ministre. Mais la CNCTR n'a aucun pouvoir pour s'y opposer. Elle peut uniquement indiquer au Premier Ministre qu'elle considère que la technique demandée serait illicite puis, si le Premier Ministre l'autorise toutefois, saisir le Conseil d'État pour s'opposer à la mesure. Sa saisine du Conseil d'État ne suspend pas la mise en œuvre de la mesure, la décision de celui-ci qui pouvant être rendu bien plus tard (la loi n'impose pas de délai fixe).

73 Ainsi, en pratique, aucune autorité indépendante n'a le pouvoir d'empêcher que des renseignements ne soient collectés en violation de la loi. Aucune « demande motivée » n'est jamais faite auprès de la CNCTR, qui est surtout spectatrice et ne peut prendre aucune décision contraignante. Au mieux, la CNCTR peut intervenir une fois que l'atteinte à la protection de ces données a été réalisée, pour demander au Conseil d'État la suppression d'informations qui ont déjà pu être exploitées illégalement. L'action de la CNCTR **intervient systématiquement après la collecte** des données : il ne s'agit pas d'un contrôle préalable.

74 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, permettent à un État de déroger à l'article 5 de la directive 2002/58 par des mesures qui ne sont soumises à l'autorisation préalable d'aucune autorité indépendante de l'entité qui les réalise et les demande.

2.6.2 Le contrôle de l'utilisation ultérieure

75 Tel que vu ci-avant, l'utilisation des informations réunies au moyen des techniques de renseignement n'est soumise à aucun cadre juridique ni à aucun contrôle. Certes, une fois que les renseignements ont été collectés, l'article L822-3 du CSI prévoit que les opérations par lesquelles ils sont « transcrits ou extraits [...] sont soumises au contrôle de la Commission nationale de contrôle des techniques de renseignement », qui peut saisir le Conseil d'État pour exiger la suppression des informations transcrites ou extraites en violation de la loi. Néanmoins, ce contrôle n'est encore une fois pas un contrôle préalable. Surtout, la CNCTR perd tout pouvoir de contrôle sur l'utilisation faite des renseignements une fois que ceux-ci ont été transcrits et extraits dans des fiches et dossiers.

76 Tout au plus, comme expliqué ci-avant, l'article L822-3 prévoit que, s'agissant des renseignements collectés pour les finalités prévues à l'article L811-3, « *les transcriptions ou les extractions doivent être détruites dès que leur conservation n'est plus indispensable à la poursuite de ces finalités* ». L'article L833-6 prévoit que la CNCTR peut recommander la destruction des informations dont la conservation ne poursuit plus ces finalités. Mais ce contrôle ne concerne que la durée de conservation des informations et non l'utilisation qui en est faite. Par exemple, la CNCTR ne peut prendre aucune « mesure correctrice » si elle s'aperçoit qu'une fiche, valablement conservée pendant 1 an à fins de surveillance économique, est aussi utilisée pendant cette durée pour une toute autre finalité, notamment une finalité qui ne serait pas prévue par la loi.

77 Ainsi, aucune autorité de contrôle indépendante n'a le pouvoir de veiller à ce que les informations obtenues en application du CSI, une fois transcrites et extraites, sont utilisées dans la limite de ce qui est strictement nécessaire (d'ailleurs, puisque la loi ne précise pas les finalités que ces utilisations peuvent poursuivre, ce contrôle de proportionnalité serait en pratique impossible à réaliser).

78 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, permettent de déroger à l'article 5 de la directive 2002/58 pour collecter des données personnelles dont l'utilisation ultérieure réalisée par l'État n'est soumise au contrôle d'aucune autorité indépendante.

2.6.3 Le contrôle des échanges internationaux

79 De la même façon qu'aucune autorité de contrôle indépendante ne supervise l'utilisation des informations après leur mise en forme, aucune autorité indépendante ne contrôle le transfert à d'autres États des renseignement collectées en application du CSI. Il ne s'agit pas d'un pouvoir de la CNCTR ni d'aucune autre autorité indépendante.

80 Par ailleurs, les pouvoirs d'enquête de la CNCTR sont drastiquement réduits par l'article L833-2 du CSI, qui prévoit que, si la CNCTR peut consulter les renseignements, transcriptions et extraits dont dispose l'administration, c'est « à l'exclusion des éléments communiqués par des services étrangers ou par des organismes internationaux ». L'État

peut ainsi librement conserver et utiliser indéfiniment n'importe quelle information obtenue sur une personne, sans être soumis à aucun contrôle, du moment que cette information lui a été transmise par un service non-français.

81 Le défaut de contrôle, tant des données envoyées par la France que des données reçues de services étrangers, conduit à la situation suivante : rien n'empêche l'État d'envoyer une information qu'il a lui même collectée à un service étranger, puis de demander à ce service de lui communiquer à nouveau cette information, dans le seul but d'échapper à tout contrôle de la CNCTR. Cette seule possibilité (parfaitement réalisable en pratique et en droit) suffit à rendre entièrement virtuels les pouvoirs de contrôle que la loi prétend conférer à la CNCTR.

82 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, permettent à l'État de déroger à l'article 5 de la directive 2002/58 pour, d'une part, collecter des données personnelles dont le transferts à des États étrangers n'est soumis à aucun contrôle indépendant et, d'autre part, collecter des données personnelles auprès d'États étrangers sans que cette collecte ne soit soumise à aucun contrôle indépendant.

3 Le recours effectif contre la surveillance

83 En substance, le Conseil d'État demande à la Cour de définir si la directive 2002/58 et la Charte permettent aux États de collecter des données de connexion sans informer les personnes concernées de cette collecte, dans la mesure où ces personnes disposeraient d'une voie de recours effective contre cette mesure (troisième question dans l'affaire C-511/18).

84 Le droit de l'Union répond déjà précisément à cette question : l'information des personnes concernées est systématiquement indispensable, peu importe qu'il existe des voies de recours par ailleurs (section 3.1). Toutefois, pour être pleinement effective et utile, la réponse de la Cour de justice devra préciser que le droit français n'offre aux personnes concernées ni l'information ni les voies de recours exigées par le droit de l'Union (section 3.2 page suivante).

3.1 L'information des personnes concernées

85 Tel que vu ci-avant (section 2.1 page 3), la grande majorité des mesures de renseignement réalisées en application du CSI doivent respecter l'ensemble des dispositions prévues soit par le RGPD, soit par la directive 2016/680, selon la finalité qu'elles poursuivent.

86 Le premier paragraphe de l'article 13 de la directive 2016/680 exige que, lorsqu'une administration réalise une mesure de surveillance afin de lutter contre des infractions, celle-ci communique aux personnes concernées par ces mesures les informations suivantes :

l'identité de l'administration, les finalités de la mesure et les droits de ces personnes. Le deuxième paragraphe du même article exige la communication d'autres types d'informations, telle que la nature des données traitées.

87 Le troisième paragraphe de cet article 13 prévoit que la loi d'un État membre peut autoriser des dérogations aux obligations prévues au deuxième paragraphe, notamment pour « retarder ou limiter la fourniture des informations » qui y sont visées, mais ne permet toutefois aucune dérogation aux obligations d'information prévues au premier paragraphe, que les États doivent donc systématiquement respecter et sans retard possible.

88 Sur ces aspects, le RGPD est moins précis que la directive 2016/680. Il serait toutefois parfaitement disproportionné qu'une personne ne reçoive aucune information quant à la mesure de surveillance qu'elle subi au simple motif que cette surveillance ne soit pas prise pour lutter contre des infractions (ne soit pas soumise à la directive 2016/680) mais simplement, par exemple, à des fins économiques ou scientifiques.

89 Puisque la directive 2016/680 encadre des mesures qui concernent les situations les plus graves, les garanties minimum qu'elle offre aux personnes concernées doivent nécessairement se retrouver pour les situations moins graves que couvre le RGPD. De même, il serait disproportionné que la Charte ne prévoit pas des garanties minimum au moins aussi importantes s'agissant des mesures réalisées marginalement pour sauvegarder la sécurité nationale.

90 Dans tous les cas, l'information des personnes concernées quant aux mesures qui les visent ne sauraient en aucun cas être réalisée au-delà du « moment où cette communication n'est pas susceptible de compromettre les enquêtes menées », tel que l'exige la Cour de justice (Tele2, paragraphe 121).

91 **En conclusion**, en application de la Charte, du RGPD et de la directive 2016/680, un État membre ne peut pas prendre de mesures dérogeant à l'article 5 de la directive 2002/58 sans prévoir que les personnes concernées par ces mesures ne soient informées de l'existence de celles-ci, de l'entité qui les réalise, des finalités poursuivies et de leurs droits.

3.2 Le droit français ne prévoit pas de recours effectif

92 Contrairement à ce qu'exige le droit de l'Union, le droit français ne prévoit aucune information préalable des personnes concernées, alors que cette information est la condition nécessaire pour exercer un recours contre des mesures illicites (section 3.2.1 page suivante). De même, dans les rares cas où les personnes peuvent contester une mesure en justice, elles sont privées de l'accès aux informations qui leur permettrait de former effectivement leur recours (section 3.2.2 page suivante). Enfin, aucune voie de recours ne permet de contester les mesures de surveillance internationale, l'utilisation ultérieure des renseignement ou leurs échanges avec des services étrangers (section 3.2.3 page 19).

3.2.1 Défaut d'information préalable

93 En droit français, le CSI autorise des traitements de données personnelles sans prévoir toutefois que les personnes concernées ne reçoivent la moindre information, en aucune circonstance, quant à l'identité de l'administration réalisant cette mesure, la finalité qu'elle poursuit ou la possibilité qu'elles ont de s'opposer à cette mesure. Ignorant tout des mesures qu'elles subissent, ces personnes ne peuvent pas se défendre de celles qui seraient réalisées en violation de la loi, sauf dans l'hypothèse inhabituelle où elles penseraient être surveillées sans en avoir pourtant la preuve.

94 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, permettent à l'État de prendre des mesures dérogeant à l'article 5 de la directive 2002/58 sans prévoir que les personnes concernées par ces mesures ne soient informées de l'existence de celles-ci, de l'entité qui les réalise, des finalités poursuivies et de leurs droits.

3.2.2 Défaut d'information pendant le contentieux

95 La Cour de justice a déclaré que « une réglementation ne prévoyant aucune possibilité pour le justiciable d'exercer des voies de droit afin d'avoir accès à des données à caractère personnel le concernant [...] ne respecte pas le contenu essentiel du droit fondamental à une protection juridictionnelle effective, tel que consacré à l'article 47 de la Charte » (Schrems, § 95).

96 En application de cet article 47, elle a décidé que, par principe, « ce serait violer le droit fondamental à un recours juridictionnel effectif que de fonder une décision juridictionnelle sur des faits et des documents dont les parties elles-mêmes, ou l'une d'entre elles, n'ont pas pu prendre connaissance et sur lesquels elles n'ont donc pas été en mesure de prendre position » (CJUE, 4 juin 2013, ZZ contre Secretary of State for the Home Department, C-300/11, § 56).

97 Ce n'est que par exception que la Cour de justice estime que, si une décision a été prise sur la base d'informations potentiellement secrètes, « le juge compétent de l'État membre concerné doit avoir à sa disposition et mettre en œuvre des techniques et des règles de droit de procédure permettant de concilier, d'une part, les considérations légitimes de la sûreté de l'État quant à la nature et aux sources des renseignements ayant été pris en considération pour l'adoption d'une telle décision et, d'autre part, la nécessité de garantir à suffisance au justiciable le respect de ses droits procéduraux, tels que le droit d'être entendu ainsi que le principe du contradictoire » (même arrêt, § 57).

98 Pour cela, l'État doit prévoir « un contrôle juridictionnel effectif [...] de l'existence et du bien-fondé des raisons invoquées par l'autorité [qui] s'opposent à la communication des motifs précis et complets sur lesquels est fondée la décision en cause ainsi que des

éléments de preuve y afférents », et ce alors que « il n'existe pas de présomption en faveur de l'existence et du bien-fondé de [ce]s raisons » (même arrêt, paragraphes 58, 60 et 62).

99 En droit français, l'article L773-1 du code de justice administrative prévoit que les techniques de renseignement réalisées en application du livre VIII du CSI ne peuvent être contestées que dans le cadre d'une procédure spécifique. L'article 773-3 de ce même code prévoit que, dans cette procédure, « les exigences de la contradiction [...] sont adaptées à celles du secret de la défense nationale », ce qui implique notamment que la formation de jugement « entend les parties séparément lorsqu'est en cause le secret de la défense nationale » et que les pièces alors produites ne sont *pas débattues* par la personne qui a formé le recours.

100 L'article 413-9 du code pénal définit les informations qui « présentent un caractère de secret de la défense nationale » comme celles « qui ont fait l'objet de mesures de classification ». L'article R2311-6 du code de la défense définit cette mesure de classification comme relevant entièrement du pouvoir discrétionnaire de l'administration : « dans les conditions fixées par le Premier ministre, les informations et supports classifiés au niveau Secret-Défense ou Confidentiel-Défense, ainsi que les modalités d'organisation de leur protection, sont déterminés par chaque ministre pour les administrations et les organismes relevant de son département ministériel ».

101 La seule procédure dont dispose une juridiction pour obtenir la déclassification d'une information et sa communication aux personnes ayant formé un recours contre une mesure de renseignement est celle prévue aux articles L2312-4, L2312-7 et L2312-8 du code de la défense. Cette procédure se déroule en trois étapes : la juridiction demande la déclassification d'une information à l'administration qui l'a classifiée ; la Commission du secret de la défense nationale (CSDN) est saisie de cette demande et transmet à l'administration son avis quant à la réponse à donner ; l'administration répond à la demande de la juridiction en joignant l'avis de la CSDN. Rien n'empêche l'administration de s'écarter de l'avis de la CSDN, qui n'est pas contraignant, et rien ne permet à la juridiction de s'opposer au refus de l'administration.

102 En résumé, l'administration peut, seule, sans contrôle et sans possibilité pour le juge de s'y opposer, exclure du débat contradictoire des informations qui ont fondé sa décision. Pas même l'avocat de la personne formant le recours ne peut y avoir accès. Le fait que la juridiction ait, elle, accès aux informations classifiées et puisse « relever d'office tout moyen », tel que le prévoit l'article 773-5 du code de justice administrative, ne corrige en rien la situation : l'absence de toute procédure contradictoire ne saurait jamais être corrigée par une procédure inquisitoire, quelqu'elle soit.

103 Enfin, les article L773-6 et L773-7 du code de la justice administrative prévoit que la personne ayant formé un recours n'est, au moment de la décision juridictionnelle, informée « d'aucun élément protégé par le secret de la défense nationale » ou, si la juridiction n'a constatée aucune mesure illicite, n'est simplement pas informée de l'existence ou non d'une mesure réalisée à son encontre ni des raisons de la licéité de celle-ci, si elle existe. Dans ces conditions, aucune personne formant un recours contre une mesure de renseignement, ni aucun des avocats qui peut l'assister, n'a connaissance des décisions passées et de la jurisprudence de la formation de jugement spécialisée saisie. Sa demande, qui ne peut déjà pas se baser sur les informations exclues par l'administration, ne peut pas non

plus se baser sur des informations passées et contextuelles. En vérité, rien n'empêche l'administration de veiller à ce que sa demande ne puisse se baser sur aucun élément factuel ou juridique, la forçant à produire une saisine blanche, sans argumentation possible.

104 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte, du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, permettent à l'État de prendre des mesures dérogeant à l'article 5 de la directive 2002/58 sans prévoir que les personnes concernées par ces mesures ou leur avocat n'aient accès, au moment de les contester devant une juridiction, aux informations sur la base desquelles cette mesure a été autorisée ni aux décisions préalablement rendues par cette juridiction.

3.2.3 Défaut de recours

105 L'exigence d'un recours effectif prévue à l'article 47 de la Charte est reprise à l'article 54 de la directive 2016/680, qui exige que « *Les États membres prévoient que, sans préjudice de tout recours administratif ou extrajudiciaire qui leur est ouvert, notamment le droit d'introduire une réclamation auprès d'une autorité de contrôle en vertu de l'article 52, une personne concernée a droit à un recours juridictionnel effectif lorsqu'elle considère que ses droits prévus dans les dispositions adoptées en vertu de la présente directive ont été violés du fait d'un traitement de ses données à caractère personnel effectué en violation desdites dispositions* ». L'article 79, §1, du RGPD prévoit une disposition identique. Ces exigences ne connaissent aucune forme d'exception.

106 Pour rappel, l'article 15 de la directive 2002/58 prévoit que les États membres ne peuvent porter atteinte aux garanties prévues à son article 5 que dans le respect des principes généraux du droit de l'Union, définis tant par la Charte que par la directive 2016/680 et le RGPD, et dont le droit à un recours effectif est l'un des plus importants.

107 Pourtant, en droit français, la licéité des mesures de surveillance de masse du contenu et des données de connexion des communications émises vers ou reçues depuis l'extérieur du territoire français (prévues à l'article L854-2 du CSI) ne peut jamais être contestée devant une juridiction par les personnes qui la subissent. Le Conseil constitutionnel l'a d'ailleurs reconnu sans aucune nuance : « la personne faisant l'objet d'une mesure de surveillance internationale ne peut saisir un juge pour contester la régularité de cette mesure » (décision n° 2015-722 DC du 26 novembre 2015, point 18).

108 Tout au plus, l'article L854-9 du CSI prévoit que la CNCTR, seule, a le pouvoir de contester ces mesures devant une juridiction, tout en étant entièrement libre de le faire ou non. Ici encore, l'absence de toute procédure contradictoire ne saurait jamais être corrigée par une procédure inquisitoire, quelqu'elle soit.

109 Par ailleurs, puisque ni l'utilisation par l'administration des renseignements mis en forme, ni leur obtention auprès d'autorités étrangères, ni leur transfert à ces dernières n'est soumis au moindre cadre juridique (tel qu'exposé section 2.5 page 11), ces mesures de renseignement sont elles-aussi impossibles à contester devant une juridiction.

110 **En conclusion**, afin de ne laisser aucune ambiguïté quant à l'interprétation de la Charte,

du RGPD et de la directive 2016/680, la Cour de justice doit déclarer comme étant contraires à ces normes des dispositions nationales qui, telles que celles prévues en droit français, permettent à l'État de prendre des mesures dérogeant à l'article 5 de la directive 2002/58 sans prévoir que les personnes concernées par ces mesures ne puissent en contester la licéité devant une juridiction.